2013-01-01

On-scene triage open source forensic tool chests: Are they effective?

Shiaeles, S

10.1016/j.diin.2013.04.002
Digital Investigation

Digital Investigation 10 (2013) 99–115

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

On-scene triage open source forensic tool chests: Are they effective?

Stavros Shiaeles [a], Anargyros Chryssanthou [b], Vasilios Katos [a,*]

[a] Information Security and Incident Response Unit, Democritus University of Thrace, 67100 Thrace, Greece
[b] Hellenic Data Protection Authority, Greece

ARTICLE INFO

Article history:
Received 14 January 2013
Received in revised form 31 March 2013
Accepted 1 April 2013

Keywords:
Triage
ACPO principles
Open source
Incident response
TriageIR
Kludge
TR3Secure

ABSTRACT

Considering that a triage related task may essentially make-or-break a digital investigation and the fact that a number of triage tools are freely available online but there is currently no mature framework for practically testing and evaluating them, in this paper we put three open source triage tools to the test. In an attempt to identify common issues, strengths and limitations we evaluate them both in terms of efficiency and compliance to published forensic principles. Our results show that due to the increased complexity and wide variety of system configurations, the triage tools should be made more adaptable, either dynamically or manually (depending on the case and context) instead of maintaining a monolithic functionality.

1. Introduction

Triage is a term deriving from medicine. According to the Free Merriam-Webster dictionary it is defined as "the sorting of and allocation of treatment to patients and especially battle and disaster victims according to a system of priorities designed to maximize the number of survivors". In a similar manner, in incident response (Brownlee and Guttman, 1998) triage is defined as the stage where a security expert assesses an incoming report about a security incident, prioritizes it, relates it to other ongoing incidents and deems whether the report is valid. From these definitions it can be evident that the overall success of a digital investigation is heavily influenced by the early actions of the first responder. Correct prioritization and handling of the live system may offer the key to an encrypted partition, or might reveal the valuable remote IP.

In this paper we used three widely available open source triage tools as a vehicle to study and understand the issues surrounding digital triage processes. We study the effort required and the practical challenges a responder may face and evaluate these tools against the requirements set out by a published practice guide for digital forensics. Having employed some of these tools in real case situations where we had to modify them on the field, we included a secondary goal in this paper which is to propose ways of improving these tools.

This paper is structured as follows. In Section 2 we present the current state of the art and research directions on triage tool requirements. In Section 3 we describe the methodology for our empirical evaluation and introduce the three tools. Section 4 reports on the evaluation of the tools with further discussion on their advantages and drawbacks summarized in Sections 5 and 6 respectively. The evaluation of the tools is continued in Section 7, where we assess the tools' compliance to an appropriate forensics principle. Finally, Sections 8 and 9 conclude with further suggestions, discussion and future work.

* Corresponding author. Tel.: +30 25410 79754.
E-mail addresses: shiaeles@ee.duth.gr (S. Shiaeles), achrysanthou@dpa.gr (A. Chryssanthou), vkatos@ee.duth.gr (V. Katos).

1742-2876/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.diin.2013.04.002

2. Background and related work

When an incident is being reported, digital forensics processes are called upon to examine the incident, collect and analyze digital evidence in order to assess the nature of the incident, identify a potential perpetrator and maybe establish whether a cyber-crime has been committed. A bug that causes a server to hang will be an incident response scenario where no human perpetrator is actually involved. However in a website defacement case for example, the collection of evidence from the underlying live system may be necessary, since potentially malicious processes may still be resident in memory. In such case digital triage forensics will be required in order to investigate the digital crime scene and collect evidence based on the order of volatility, as defined in RFC 3227 (Brezinski and Killalea, 2002). "Digital Triage Forensics (DTF) is defined as a procedural model for the investigation of digital crime scenes including both traditional crime scenes and the more complex battlefield crime scenes" (Pearson and Watson, 2010). Rogers et al. (2006) define a computer forensics triage model (CFFTPM) as "investigative processes that are conducted within the first few hours of an investigation and provide information used during the suspect interview and search execution Phase". The goal is to identify useful evidence while at the crime scene in order to guide the investigators and help them identify both other potential evidence, which might be "hidden in plain sight", as well as assess the perpetrator's "danger to society". As triage is part of the digital forensics life cycle and involves the collection of evidence that may be later presented in a court of law, the adherence of all employed triage tools and processes to forensic principles ensuring the admissibility of the collected evidence is non questionable. A typical and well developed set of principles is described in the well known Association of Chief Police Officers (ACPO) Good Practice Guide for Computer Based Electronic Evidence (ACPO, 2008). The guide comprises of four Principles which are rather generic in order to be easily understood and followed in many circumstances. More specifically, Principle 1 states that "No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court." However, where a live system is involved or the need arises to access original data held on a computer or on storage media Principle 2 states that the investigator accessing the live system or the original data "must be competent to do so and be able to give evidence explaining the relevance and the implications of his actions". In each and every case an audit trail of all processes applied to computer-based electronic evidence must be created and preserved (Principle 3). Consequently the digital forensics triage tools have to be able to keep an audit trail of their actions, so that a) an independent third party can follow them up and end up with the same result b) the investigator can explain how these tools are relevant to his investigation and how they changed the examined system without setting his investigation in danger. At the same time these tools have to be able to collect evidence beginning from the volatile to the less volatile (Brezinski and Killalea, 2002) while collecting as many forensic artifacts as necessary. A good resource on potential forensic artifacts is the ForensicArtifacts.com database and SANS resources such as the Sans-Digital-Forensics-and-Incident-Response-Poster-2012 (Lee, 2012) or Sans forensic cheat sheets, where an investigator can find a wide variety of evidence that he has to look for, depending always on the type of investigation (in an internet-related crime for example the focus would be on the suspect's browsing habits and history), as well as the tools he can utilize (in the internet-related crime example Nirsoft's web browsers' tools package might be useful).

Rogers et al. (2006) in their proposed triage process model highlight the importance of prioritization prior to moving into the collection of the various system and user data. Emphasis is given on the data that have short time to live such as routing tables, processes and temporary files. The authors conclude that forensic examiners need a repertoire of tools as there is no tool that can weight all possible technical and legal considerations a first responder may face in a specific case. This suggests that the triage tool will need to be flexible and maintain the ability to respond to the evidence during collection by changing its acquisition behavior.

An important trait of a triage tool is the requirement to collect data in a relatively short time window. This is often overlooked in practice as the tools are becoming complex in order to preserve as much information as possible, later to be used in analysis. Horsman et al. (2011) attribute this drawback to the fact that triage tools are descendants from traditional forensic tools that are designed to perform a post mortem analysis. We argue that in order to achieve a suitable tradeoff between the speed of the triage process and the appropriateness of the collected data, the triage tool needs to have adaptiveness capabilities. SPEKTOR triage tool for example attempts to support some degree of automation, but this is done in order to be used by people with no particular technical abilities. This is in clear violation of ACPO's second principle and as such we consider it to be a poor practice. In fact, we argue that a triage tool will need to support automation in order to simplify the first responder's work, but this should not be done by sparing the expertise and skills of the responder.

A key dilemma in incident response is the decision to perform a complete memory acquisition versus a live response. Memory acquisition can be very informative but is rather slow. In addition, memory acquisition will take a snapshot of the execution state of the system and the analyst will not have the opportunity to perform some further acquisition based on the findings. Yet, hardware evolution leads to ever increasing memory sizes suggesting that a memory image may provide information of past and completed processes which cannot be mined through live response tools (Aljaedi et al., 2011). Live response on the other hand can be very effective if the first responder is well prepared on the underlying case. However, it requires a portfolio of tools that are typically executed from a script. In addition the tools need to be configured in order to be compatible with the suspect system. Waits et al. (2008) conclude that both approaches should be followed, with the incident response tools fulfilling the role of the triage phase, collecting the minimal information possible in order to allow further planning. Once more, minimal information requires well preparation and customization of the triage tool.

From the above discussion it is evident that a triage tool needs to balance a number of requirements in terms of performance, complexity and adaptability. In the following sections we put three open-source triage tools to the test, assess their behavior and reach to a series of conclusions as to their ability to meet the expectations of the first responder.

3. Methodology

For our primary research we tested the ***TriageIR***, ***TR3Secure*** and ***Kludge*** triage/incident response tools. We examined their behavior in various Microsoft Windows operating systems and compared the results that they produce. We focused on Microsoft's Windows operating systems as, according to statistics, MS Windows type OS remains the most popular operating system used by home users (Netmarketshare, 2012).

For our primary research we setup a testbed that included machines running various MS Windows OS that a typical home end user would use.

3.1. Testbed setup procedure

The base host operating system was Windows 7 SP1 64-Bit with Quad Core, 8 GB RAM and 2 TB Hard Disk. On this Host VMware Player 8 was installed. Subsequently 8 virtual machines (VMs) were created according to the specifications summarized in Table 1.

Initially each created VM was loaded with a default installation of a Windows OS system (XP SP3 32 bit, XP SP2 64 bit, 7 32 bit, 7 64 bit, 7 SP1 32 bit, 7 SP1 64 bit, 8 32 bit and 8 64 bit). Following the installation of the OS on the VM, we installed Sandboxie 3.74, in order to be able to execute the triage tools in sandboxed environment. Sandboxie could be installed on all VMs except Windows XP 64 bit, where we encountered an incompatibility, as Sandboxie is not supported in such OS. As a next step we copied TriageIR v.79, Kludge-3.20110223 and TR3Secure on our "E: disk" which served as an external USB drive following our test scenario. This is a typical setting where the forensic examiner or first responder introduces an external USB drive to the system in order to run his triage tools and collect the incident data. Furthermore, in Windows 7 64 bit and Windows 8 64 bit we had to modify Sandboxie's configuration file (Sabdboxie.ini) and change the value of DropAdminRights from y to n, in order to be able to run some programs that are part of the triage tools and can only produce results if run under administrator privileges. This setting is required due to changes in the kernel of Windows 64 bit operating systems. It should be noted that *"DropAdminRights is a sandbox setting in Sandboxie.ini, which specifies whether Sandboxie will strip Administrator rights from programs running in the sandbox"*.

Our testbed is depicted in Fig. 1 below.

3.2. Testing triage tools

Table 1
Virtual machine hardware specifications.

Network mode	C disk for MS Windows	E disk for triage tools	RAM	CPU Cores
Bridge	60 GB	10 GB	1 GB	2

All tools were tested with all their options enabled and in two different execution modes; sandboxed environment and "normal" execution. We utilized a sandboxed environment in order to find out which files are created in the examined system's hard disk and investigate how the integrity of the examined system is being affected. We executed the tools in "normal" execution mode in order to see how the tools actually perform when not restricted in an isolated "sandboxed" environment. For the Windows 7 and Windows 8 OS (32 bit and 64 bit) it was necessary to enable for all the tools the "Run as administrator" option, as UAC prevented some programs, such as win32dd.exe and Memoryze.exe (programs that image the system's memory in dd format) called by the tools, from running correctly.

3.2.1. TriageIR v.0.79

The first tool that we tested was TriageIR v.0.79. According to the documentation manual, TriageIR needs the following tools added in a folder named "tools", residing in the program's folder, in order for it to run correctly. These tools are: a) DumpIt memory utility, b) Sysinternals Suite, c) RegRipper, d) md5deep and sha1deep, e) 7Zip Command Line.

The "tools" folder structure should look like as in Fig. 2.

After all the tools were placed in the respective folders we executed the "Triage – Incident Response.exe". The tool provides 6 tabs – "pages" containing a variety of options concerning System Information (see Fig. 3), Network information, and so forth. In order to fully assess the tool's functionality we executed it with all its options marked in our two test modes.

In the sandboxed environment TriageIR produced some errors when it tried to load some drivers (ex. the win32dd.sys used by win32dd.exe in order to create a memory dump). This behavior is normal, as "programs running under the supervision of Sandboxie are stripped of privileges required to start drivers",[1] thus resulting in less data being collected, as the tools associated with these drivers and services do not function properly (the tools crash). In normal mode the tool executed smoothly in every different operating system and collected incident data in a folder that is automatically created. This folder is in the same location where we execute the Triage – Incident Response.exe, which in our case is on the E: disk. The tool failed only in Windows 8 OS 64 bit, where the win64dd.exe program cannot be loaded resulting in the system's memory image not being collected. However we observed that win64dd.exe stops failing if the execution of TriageIR is interrupted by the user once or twice and then executed again (always as Administrator or with UAC disabled). We conjecture that this problem exists in Windows 8 64 bit due to changes in the operating system's kernel.

3.2.2. TR3Secure

Next in our tests was the TR3Secure data collection script. The tool uses a .bat script to call a series of tools that are either native Windows tools, located in the Windows\System32 folder, or tools that need to be downloaded from the Internet and placed into a folder named "tools", which resides in the tool's folder (Fig. 4). Additionally, a text

[1] http://www.sandboxie.com/index.php?SBIE2103.

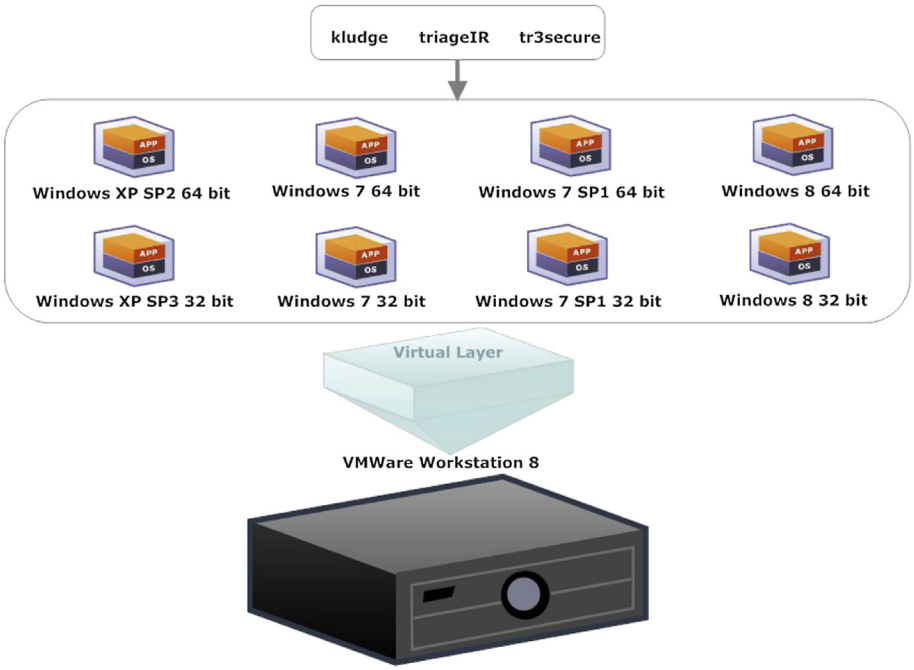

Fig. 1. Triage testbed setup.

file which is named diskpart_commands.txt and contains specific commands in separate lines (list disk, list volume) needs to be created in the "tools" folder with specific commands placed on separate lines. The "tools" folder structure is depicted in Fig. 5.

We carried out our testing procedure selecting option 4 from the tool's menu (see Fig. 6) in order to use all available capabilities. We used a slightly modified version of the tool's .bat script, which entailed some minor corrections (see Appendix A.2).

The .bat script met most expectations in all operating systems, but we noticed some issues in 64-bit systems, as some of the utilities invoked by the tools are not compatible with such systems. In addition we had to modify the code in this script relating to the path of the tools in Windows 7 and Windows 8 32-bit and 64-bit in order for it to succeed in locating the tools. It should be noted though that the script will not need such code modification if it is run through a trusted command prompt shell – that is a shell running from the investigator's USB drive. In 64-bit operating systems a memory image could not be collected possibly due to the fact that Memoryze is not supported in a 64-bit OS.

RegRipper	13/10/2012 8:59 μμ	File folder	
sleuthkit-win32-3.2.3	13/10/2012 8:59 μμ	File folder	
SysinternalsSuite	13/10/2012 2:34 μμ	File folder	
7za.exe	18/11/2010 3:27 μμ	Application	574 KB
cmd.exe	17/4/2012 1:35 πμ	Application	1.232 KB
DumpIt.exe	22/10/2011 3:41 μμ	Application	203 KB
md5deep.exe	13/7/2011 5:58 μμ	Application	58 KB
md5deep64.exe	26/7/2011 2:46 πμ	Application	52 KB
robo7.exe	20/11/2010 12:25 μμ	Application	125 KB
robocopy.exe	18/4/2003 10:06 μμ	Application	78 KB
sha1deep.exe	26/7/2011 2:46 πμ	Application	62 KB
sha1deep64.exe	26/7/2011 2:46 πμ	Application	56 KB
win32dd.exe	1/1/1980 3:00 πμ	Application	97 KB
win32dd.sys	1/1/1980 3:00 πμ	System file	53 KB
win64dd.exe	1/1/1980 3:00 πμ	Application	108 KB
win64dd.sys	1/1/1980 3:00 πμ	System file	60 KB

Fig. 2. TriageIR v.0.79 Tools Folder.

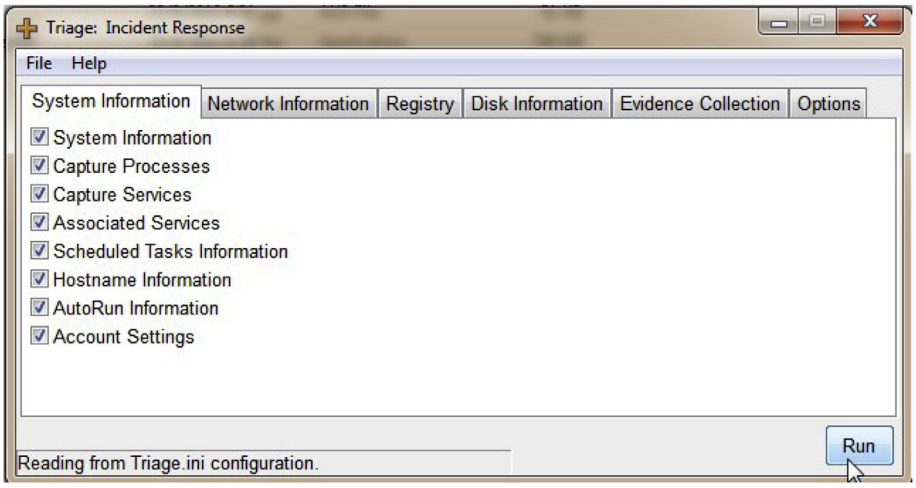

Fig. 3. TriageIR v.79 GUI.

Fig. 4. TR3Secure main folder structure.

3.2.3. Kludge 3.20110223

Lastly, we tested Kludge-3.20110223. Kludge is created with the idea of being run remotely through a network by using the administrative shares in the target pc. In this way, it copies all the files required by the tool to the remote computer and then it runs them in order to collect the required data. This could be considered a poor digital forensics practice as the tool makes many modifications to the hard disk of the remote computer. Additionally, if remote administrative shares are disabled in the Windows remote system then the tool cannot be executed without the investigator enabling them. Thus, in order to keep our initial setup, which entailed running triage tools from an external USB drive and the investigation data being saved in the same drive, we modified the Kludge.bat file. This .bat file is the tool's main executable file and is located in the kludge-3.20110223.zip file. The kludge-3.20110223.zip file contains the kludge.zip file, which, as the tool is designed, is uploaded to the remote machine and afterwards unzipped to a temp folder (C:\WINDOWS\Temp\analysis\). Following our modifications the script could run from our external USB disk without any issues and store the collected incident data to the same disk (see Fig. 7 and Appendix A.1 for a link to download our modified code). From there onwards, the procedure we followed did not differ from the other two tools described earlier.

4. Results

In order to evaluate the effectiveness of the triage tools with respect to the order of volatility firstly we have to define what the order of volatility is for a typical system, based on RFC3227 (Brezinski and Killalea, 2002), and secondly we have to define each scale in the order of volatility hierarchy. CPU registers and cache represent the most volatile state of data as these locations change most frequently (typically in an order of milliseconds). Memory is the source of a wealth of information such as running processes, open connections, thus it is best that memory is imaged with minimum alterations. Next in line are data kept in the memory such as process tables, which can help direct an investigation, when a "suspicious" process is noted. A temporary file system can be defined as a file location, such as the Windows\Temp folder, where programs load temporary files, which are later on deleted or "forgotten" when the programs terminate. Storage media such as hard disks contain a wealth of information and are not altered as easily as the previous described items. Remote logging data is data that can be collected, for example, from IDS sensors or from the examined system itself and can help the investigator identify what the system under examination was doing at the time of acquisition or before. As these data reside in different devices, it is not so easy to be altered either by the investigator's tools or by malicious software running in the system under examination.[2] Physical configuration and network topology constitute more long term and less volatile data that can be gathered at a later stage as they are not so changeable. The

[2] See http://help.papertrailapp.com/kb/configuration/configuring-remote-syslog-from-windows for examples on how to remotely log windows OS.

Fig. 5. TR3Secure "tools" folder structure.

same applies to archival media such as cd-roms, dvds, and so forth.

In Table 2 we present a consolidated view of the incident data that these tools were able to collect as part of the triage process. The table column headers represent the order of volatility scale, while the row headers represent the tested tools.

As depicted in Table 2, quite expectedly none of the tools collect evidence from registers and cache, since collecting this type of data maybe has barely some meaning in triage processes. This in part has to do with the fact that the content of CPU registers, for example, is difficult to be analyzed. All of the tools collect the routing table and the ARP cache, whilst preserving other data such as Netbios-related data (general information and sessions), active connections, network adapter information, DNS information and other. All of the tools collect significant amount of information on processes, such as running processes and process file handles. TR3Secure collects kernel statistics, while all the tools collect information relating to the kernel build. All of the tools image the system's memory, whilst preserving Prefetch files. Two of the tools (TriageIR, Kludge) collect registry files, in unprocessed format (.reg, .dat, .hiv, .log files) and in processed format (.txt files produced using Regripper). All tools collect data on users' activity (locally-logged-on-users, active-logon-sessions), whereas two of them (TriageIR, TR3Secure) collect clipboard contents. In addition TriageIR also collects recent and jump lists files and Kludge collects NTFS data streams.

With regards to temporary file system acquisition, two of the tools (TriageIR, Kludge) collect system event logs (.evt files), with one of them acquiring .evtx files also. In practice the tools only collect .evt event logs, since during our tests TriageIR failed to collect any .evtx event log files (in Windows 7 or Windows 8 OS). In addition Kludge also collects antivirus logs pertaining to specific vendors (McAfee and Symantec) and sometimes specific software versions. Acquiring a hard disk image has no meaning during the triage process, as a hard disk image is something that needs to be analyzed later in a lab, with the same applying to archival media.

Regarding remote logging and monitoring data, TriageIR collects open shared files information, whereas TR3Secure collects information on remotely-logged-on-users and remote-users-ip-addresses. Concerning physical configuration and network topology, all tools collect a variety of data on system configuration (hardware and software-wise).

In Table 3 we summarize the tool effectiveness for every operating system. A tool is considered "effective" if it performs without any errors and collects all the data according to the prescription of the order of volatility. A tool is considered "medium effective" if it produces a few errors, when executed, but collects most of the data that the order of volatility prescribes. A tool is considered "less effective" if it produces a large number of errors when executed. A tool is considered "ineffective" if it fails to collect vital evidence (memory for instance) that the order of volatility prescribes. As depicted above, TriageIR is deemed "medium effective" in all operating systems as it produces a few errors during execution resulting in some incident data not being collected. It is worth noting that TriageIR is not Windows 8 ready as it encounters problems in some of the utilities (win64dd.exe, at.exe) that it uses due to deprecation or incompatibility of these utilities with the latter OS. TR3Secure is deemed "medium effective" in 32-bit operating systems and "ineffective" in 64-bit operating systems, as in 64-bit OS it fails to acquire the system's memory. It is worth noting that TR3Secure collects less data than the other two triage tools. Kludge is deemed "medium effective" in Windows XP 32-bit operating system and "less

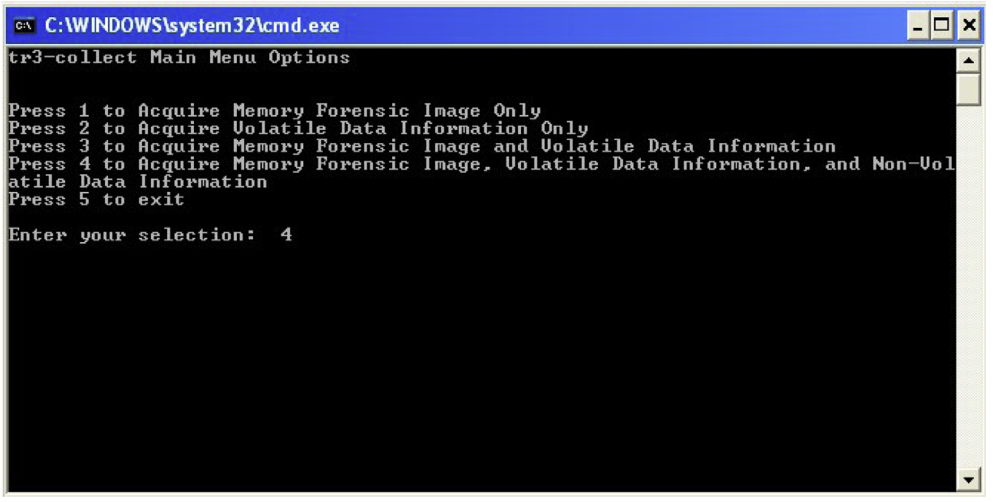

Fig. 6. TR3Secure Main Menu.

effective" in the other Windows OS, because the version of "Hobocopy" included in the downloadable Kludge package and used to copy, for example, event logs, is not supported in OS other than Windows XP 32-bit. Thus, a significant amount of incident data is not collected.

In Table 4 a consolidated view of the modifications performed by each tool on the registry and file system of the corresponding OS is presented. All the modifications were recorded by using a) Buster Sandbox Analyzer 1.87 (BSA) in conjunction with Sandboxie and b) Sandboxie in a standalone setting. The number of modifications depicted below is a rough estimate as Sandboxie itself reports that, for example, "*Windows may store copies of programs files in the Prefetch folder even when the programs were executed under Sandboxie*",[3] which means that BSA will not log files such as Prefetch as part of the file system modifications. The same applies to event log and potentially other files. It is worthwhile noting that the modified version of Kludge was the most consistent over all systems and the most "forensically friendly" of all three tools. More information on the critical modifications can be found in the Sandbox analyzer log snippets in Appendix C.

5. Advantages

5.1. TriageIR 0.79

TriageIR collects information about the examined computer's startup process which can be proven useful for malware analysis. Specifically, it utilizes the "wmic startup list full" command which "*shows a whole bunch of stuff useful in malware analysis, including all files loaded at Startup and the reg keys associated with autostart*" (Skoudis, 2006). Additionally it locates and copies all usrclass.dat files, files that represent each user's profile settings, by using sleuthkit's ifind and icat commands. Moreover the tool rips all registry hives, by means of the Regripper utility. Another advantage of TriageIR is the fact that it produces MD5 and SHA-1 hashes of evidence files (logs, Prefetch, recent links, jump lists and registry files). This functionality can be used to prove the integrity of the evidence data. Finally, the tool creates a compressed file of the produced incident report (excluding .dat1 files, .ini files and empty folders) in .7z format using ultra compression.

5.2. TR3Secure

From a forensics practice perspective TR3Secure includes the desirable functionality as it provides the first responder with the capability to set a) case identifier, b) analyst's name, c) drive letter for the volume storing the tools, d) drive letter for the volume to store the collection data, e) current date and time. Additionally it logs every step of the triage process apart from the produced errors and it runs through a single command shell window, allowing the examiner to observe any occurring errors.

5.3. Kludge 3.20110223

Kludge collects digital evidence that the other two tools do not. First of all, it collects internet browsers history from Mozilla Firefox and Internet Explorer, which can be proven very useful if, for example, the examiner is working on a case relating to a plethora of common offenses such as grooming, bullying, spam, and so forth. Additionally, it collects antivirus logs and reports on the firewall state. Furthermore, it collects process dumps and process-related memory for each running process.

From a forensics perspective Kludge creates timelines of system activity by using fls. This functionality can be useful for the examiner, as this type of triage report "*gives an investigator clues regarding where to probe further*".[4] Finally, Kludge produces an html file, through which the investigator can navigate the collected digital evidence. This

[3] http://www.sandboxie.com/index.php?PrivacyConcerns.

[4] http://wiki.sleuthkit.org/index.php?title=Timelines.

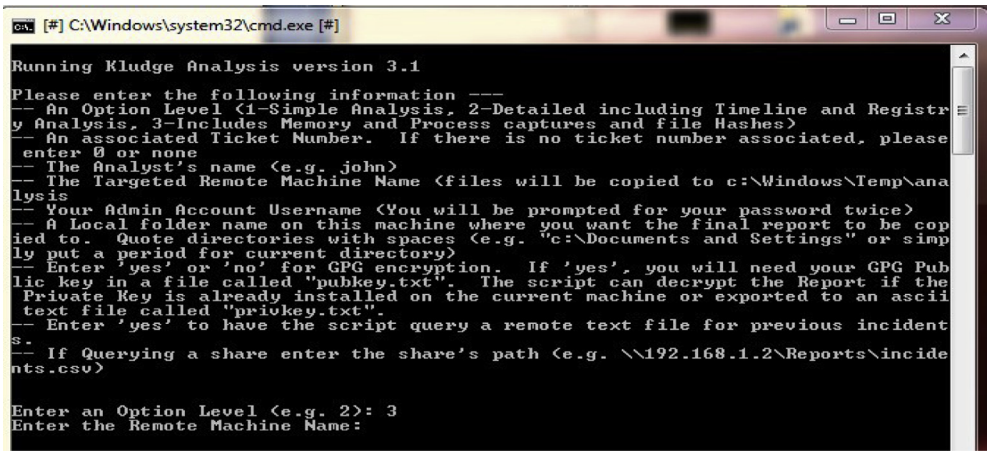

Fig. 7. Kludge script execution.

simplifies the work of the investigator and potentially speeds up the triage process.

6. Drawbacks

None of the triage tools state in their manuals that the examiner has to employ for all the tools the "Run as administrator" function in Windows Vista, 7 and 8 operating system environments, as UAC prevents some programs, such as those that collect memory, from running correctly.

6.1. TriageIR 0.79

TriageIR presents some design errors that might be caused by programming faults or incompatibility of the utilities the tool uses in various operating systems. First of all, the tool does not collect any Netbios information, as the Nbtstat command utilized by the tool for this specific purpose seems to fail in all tested operating systems. Additionally, the tool collects partial event log information in Windows 7, 8 and XP 64-bit operating systems, as robo7 utility fails to copy .evtx files in Windows 7 and 8 due to incompatibility, while the tool's author seems to have not catered for collecting event log files in Windows XP 64-bit operating systems. Moreover, the tool does not collect the security registry hive in Windows XP, as the operating system does not allow the administrator to "*navigate his way through the HKLM\SECURITY hive*"[5] by default resulting in the tool not being able to collect the hive in question due to access restrictions. The tool does not record the hard disk's directory structure in Windows XP 64-bit, although the command utilized (tree c:\ /f /a) is seemingly correct. The tool also fails to collect, although so designed, various information from the examined computer (hosts file, current logon user, user logons and firewall configuration). This is due to the fact that the tool's author has omitted to call the functions collecting this information through the tool's GUI. In order to correct this omission, the author has to a) create the appropriate checkboxes in the tool's graphical interface (through the tool's TriageGUI()), b) correlate the Firewall, Hosts and LoggedOn .ini settings with the corresponding checkboxes in the tool's GUI (through the tool's Ini2GUI()) and c) call the appropriate functions ("Firewall", "Hosts", "LoggedOn") through the tool's INI2Command(). It should be noted here that the LoggedOn function calls the logonsessions utility by using the command "logonsessions -accepteula c", which is not correctly syntaxed thus unable to execute. Furthermore, the tool fails to collect Prefetch files in Windows 7 64-bit with no service pack installed. The tool leverages the command whoami to collect current user info. However, this command does not function in Windows XP, unless Windows XP SP2 support tools are installed. Lastly, scheduled tasks data are not collected in Windows 8, as the utilized AT command has been deprecated and the user is advised by the operating system to use schtasks.exe instead.

By inspecting the execution and results, the tool seemed to violate a number of expectations on forensic soundness. First of all the tool utilizes Sysinternal's ntfsinfo utility to record ntfs information. The utility requires as a parameter a hard disk partition letter in order to operate. TriageIR takes for granted that the examined windows partition letter is c: and attempts to read ntfs info on that partition. If Windows OS is not installed on the c: partition ntfsinfo will not collect any ntfs information regarding the operating system partition. The same applies to the usage of absolute paths (C:\Users\, C:\Documents and Settings\) for the collection of user profiles (USRClass.dat files), recent links, jump lists, event logs and directory structure. Furthermore, the tool adds registry keys required for the execution of the Sysinternals tools but does not seem to undo these registry alterations. Additionally it does not record all executed commands in the created incident log file. As such, the examiner is not in a position to know which commands executed correctly, which failed and why. Traceability of the execution becomes even more difficult as the tool calls a separate command shell for each utility invoked, which

[5] See http://en.wikipedia.org/wiki/Windows_Registry for information on Registry in general and http://www.registryonwindows.com/registry-security-1.php in regards to the HKLM\SECURITY hive in particular.

Table 2
Tested tools – collected forensic artifacts vs. order of volatility scale.

Order of volatility (from more volatile to less volatile) ↓		TriageIR 0.79	TR3Secure	Kludge 3.2
Registers and Cache	No data collected	X	X	X
Routing table, arp cache,	Network-related data → ARP cache	X	X	X
process table, kernel	Network-related data → Routing table		X	X
statistics, memory	Network-related data → DNS cache and resolution		X	
	Network-related data → DNS Information	X		X
	Network-related data → A records			X
	Network-related data → Host file			X
	Network-related data → Netbios routing table	X		X
	Network-related data → Netbios information (sessions, connections, file transfer over netbios)	X	X	X
	Network-related data → Port to process mapping		X	
	Network-related data → TCP/UDP active connections	X	X	X
	Network-related data → TTL			X
	Network-related data → Firewall (info, status)			X
	Process data → Process File Handles	X	X	X
	Process data → Running Processes-DLLs	X	X	X
	Process data → Services			X
	Process data → Process to exe mapping		X	
	Process data → Process to user mapping		X	
	Process data → Child processes		X	
	Process data → Process dependencies		X	
	Process data →Process dumps			X
	Process data → Process memory			X
	User's activity → Active logon sessions		X	
	User's activity → Logged on users	X	X	X
	User's activity → Recent files	X		
	User's activity → Internet browsers history			X
	User's activity → Jump lists Files	X		
	User's activity → Clipboard-contents		X	X
	Registry hives → Sam	X		X
	Registry hives → Security	X		X
	Registry hives → System	X		X
	Registry hives → Software	X		X
	Registry hives → HKCU	X		X
	Registry hives → NTUSER.dat	X		X
	Registry hives → USRCLASS.dat	X		X
	Various timelines → IE Timeline			X
	Various timelines → FF Timeline			X
	Various timelines → Hard disk timeline			X
	Various timelines → Prefetch info			X
	Various timelines → Recycle Bin timeline and contents			X
	Memory image			X
	System configuration → VSS service status			X
	Prefetch files	X	X	
	NTFS data streams		X	X
	UnSigned-executables → Uptime		X	
Temporary file systems	System event logs → evt files	X		X
	System event logs → evtx files	X		
	Processed event logs → System	X		X
	Processed event logs → Security	X		X
	Processed event logs → Application event logs	X		X
	Antivirus logs			X
	No data collected		X	
Disk Remote logging and	Not applicable	X	X	X
monitoring data that	Network-related data → Open shared files	X		
is relevant to the	User's activity → Remotely logged on users		X	
system in question	User's activity → Remote users IP-addresses		X	
	No data collected			X
Physical configuration,	Network-related data → Network configuration	X	X	
network topology	Network-related data → Network Adapter info			X
	Network-related data → Routing table	X		X
	Network-related data → Host File	X		X
	Network-related data → Enabled network protocols		X	
	Network-related data → Promiscuous adapters		X	
	User's activity → Logged on users	X		
	System configuration → User accounts policy	X		
	System configuration → User groups		X	
	System configuration → Startup information	X	X	
	System configuration → Directory structure	X		

(*continued on next page*)

Table 2 (*continued*)

Order of volatility (from more volatile to less volatile) ↓		TriageIR 0.79	TR3Secure	Kludge 3.2
	System configuration → Mounted disks information	X		
	System configuration → Hostname	X		
	System configuration → Local shares	X		X
	System configuration → Schedule tasks	X		X
	System configuration → Kernel build	X		
	System configuration → Register organization and owner	X		
	System configuration → OS-version		X	
	System configuration → Group policy listing and RSOP		X	
	System configuration → Installed software		X	
	System configuration → Security settings		X	
	System configuration → Hardware devices		X	
	System configuration → Number of processors and their type	X		
	System configuration → Amount of physical memory	X		
	System configuration → System's install date	X		
	System configuration → System variables	X		
	System configuration → System configuration			X
	System configuration → Firewall configuration	X		
	System configuration → Services	X		
	System configuration → Type of installation	X		
	System configuration → NTFS partition info	X		
	Certain applications → Version and Signing info for Acrobat			X
	Certain applications → Acrobat Reader			X
	Certain applications → Flash			X
	Certain applications → Java			X
	Certain applications → Firefox			X
	Certain folders structure → Program Files			X
	Certain folders structure → Documents and Settings			X
	Certain folders structure → Windows			X
	UnSigned-Executables → Computer name			X
	UnSigned-Executables → Autoruns			X
	UnSigned-Executables → Startup apps			X
	UnSigned-Executables → BHO's			X
	UnSigned-Executables → Hotfixes and service packs			X
	UnSigned-Executables → Environment Variables			X
	UnSigned-Executables → Uptime			X
	UnSigned-Executables → Operating System Information			X
	UnSigned-Executables → Drive Information			X
	UnSigned-Executables → Partition info			X
	UnSigned-Executables → Users			X
	UnSigned-Executables → USB device history			X
	Registry files			X
Archival media	Not applicable	X	X	X

vanishes after execution resulting in the examiner not being able to inspect the produced errors. However, although TriageIR creates MD5 hashes of the evidence files, it does not produce similar hashes for all the reports (ex. ARP Info, Network Connections, etc.), which are created during execution. This can be justified in part, as these reports are not reproducible (in a second execution some of these reports will entail different information). However, it is our belief that the tool should create also hashes of the reports, in order to be able to maintain a proper chain of custody for all digital evidence collected or produced by the tool. Finally, if the tool's compression functionality is used, certain items (.dat1 and .ini files) are not collected.

6.2. TR3Secure

The tool exhibited a number of errors during execution. The most serious one was that it seems to run smoothly on 32-bit operating systems but it fails on 64-bit OS as some of its tools, including the one that images the memory, are built for 32-bit OS. For example, pv.exe is used to map running processes to executables, but, when run on a 64-bit OS environment, it seems to map only 32-bit running processes. In Windows 7 64-bit the tool could not find the path of the "tools" folder, thus certain variables must be defined, in order for the tool to execute correctly.

The tool, when run in OS that use a different codepage (Greek codepage 737 for example) produces text files that need to be viewed with specific viewer (for example with Wordpad), in order for the results to be viewable.

6.3. Kludge 3.20110223

Kludge presents some out-of-the-box errors that may have been caused by programming faults or incompatibility of the utilities the tool invokes in various operating systems. First of all, the Hobocopy utility which Kludge utilizes for copying certain files, crashed in

Table 3
Tool effectiveness.

Tool	Win XP SP3 32 bit	Win XP SP2 64 bit	Win 7 32 bit	Win 7 SP1 32 bit	Win 7 64 bit	Win 7 SP1 64 bit	Win 8 32 bit	Win 8 64 bit
TriageIR 0.79	Medium effective	Medium effective	Medium effective	Medium effective	Medium effective	Medium effective	Medium effective	Medium effective
TR3Secure	Medium effective	Ineffective	Medium effective	Medium effective	Ineffective	Ineffective	Medium effective	Ineffective
Kludge 3.20110223	Medium effective	Less effective	Less effective	Less effective	Less effective	Less effective	Less effective	Less effective

Windows 7 and 8 OS, 32-bit and 64-bit versions, resulting to event logs and registry files not been collected. It appears that the version included in Kludge downloadable package is old and, according to the utility's website, is destined for Windows XP 32-bit systems. In order to run the Hobocopy utility in Windows 7 and Windows 8 OS (32-bit and 64-bit versions) we had to replace the version in question with a version that supports Windows 7 and 8 and also install Microsoft Visual C++ 2010 Redistributable Package in order for the utility to execute and produce the desired results.

Additionally, "At.exe", "Netstat.exe", "Ifconfig.exe", "Arp.exe", "Route.exe", "Net.exe" and "Streams.exe" utilities invoked by Kludge in Windows 7 and 8 OS, (32-bit and 64-bit versions) crashed as these tools depend on netapi32.dll architecture, which is different in Windows 7 and 8 systems. Also, the wmic utility which parses mof files, does not execute in the aforementioned operating systems. Moreover, Kludge may collect AV logs, which is an advantage, but it collects specific AV logs (Symantec Antivirus Corporate Edition 7.5, Symantec Endpoint Protection, McAfee\VirusScan, McAfee\MSC). This is a drawback that limits this useful functionality as Symantec and McAffee share only 15% of the antivirus market (OPSWAT, 2012). This means that in at least 85% of the cases Kludge will collect no antivirus logs. It also reinforces the fact that the first responder must be fully aware of the capabilities and limitations of the triage tool he decides to employ. Additionally, Kludge does not collect .evtx files, which means that the tool does not acquire event logs in Windows Vista, 7 and 8 OS. With regards to forensic practices, the tool does not keep a detailed log of the utilities invoked making it difficult to check which utilities/commands were actually executed during the triage process.

Another peculiar feature of Kludge is that it is designed to run only remotely through administrative shares. Therefore, in order to collect data from a remote machine, administrative shares must be enabled in Windows operating systems. Another important issue is that Kludge uploads its tools to the remote machine in c:\Windows\Temp\ folder in a zipped format file and then unzips them, in order to execute them by using the wmic utility. The results, including the system's memory dump, are saved in the same folder. Provided that nowadays computer systems have at least 2 GB of RAM the examined system would significantly be altered. In addition and similar with TriageIR, the tool does not remove upon completion the registry keys it adds to the system; these registry keys relate to the execution and functionality of the Sysinternals utilities.

7. Adherence to ACPO Principle 2

Triage is inevitably linked with accessing the original data from a live system. The admissibility safeguard captured by Principle 2 suggests that the investigators accessing the live system should be competent enough and capable of explaining the relevance and implications of their actions. Consequently the investigators' competence would also be related to their understanding on how the triage tool interferes and disturbs the configuration, states of the live system and the underlying data. In the following subsections we highlight the behavior of the tools examined in this paper.

7.1. TriageIR 0.79

TriageIR modifies the hard disk of the system pertaining to the operating system it is executed in. As the tool invokes its repertoire of utilities items relating to the actual

Table 4
Summary of file system and registry modifications.

OS	Tool		
	TriageIR	TR3Secure	Kludge (modified version)
Win XP SP3	FM[a]: 39 (mainly prefetch and /system32/CatRoot) RC: 33	FM: 13 (one in /system32/) RC: 21	FM: 0 RC: 4
Win 7 64 b	FM: 84 (mainly prefetch and logfiles) RC: 379	FM: 4 (mainly logfiles) RC: 71	FM: 1 (temp appdata) RC: 6
Win 7	FM: 39 (prefetch and user appdata) RC: 134	FM: 26 (mostly in prefetch, one in /system32/) RC: 131	FM: 1 (temp appdata) RC: 14
Win 8 64 b	FM: 138 (prefetch and user appdata) RC: 354	FM: 45 (mostly in /INF folder) RC: 73	FM: 0 RC: 6
Win 8	FM: 29 (prefetch and user appdata) RC: 131	FM: 19 (2 in /system32/) RC: 127	FM: 1 (temp appdata) RC: 8

[a] **FM**: File creations/modifications – **RC**: Registry changes.

Windows OS functionality, such as Prefetch, recent files, jump lists files (Windows 7 and Windows 8), CryptnetUrlCache and temp folders, are altered. The same applies to registry keys, which are altered or added. In Windows XP SP3 32-bit, wbem logs (C\WINDOWS\system32\WBEM\Logs) are altered, whereas in Windows XP, 7 64 bit (SP1 and no SP1), 8 (32-bit and 64-bit) the event logs folder is altered. In cases where a utility crashes (Windows 7 64-bit and 8 64-bit), appcrash reports are created in a specific folder (C:\users\all users\Microsoft\Windows\WER\ReportArchive\). In all Windows OS versions, except Windows 7 64-bit SP2, files are created in the C\Windows\system32\CatRoot2\ folder, while the tool loads, in all Windows OS, a Sysinternals driver named "PROCEXP152.SYS". Similarly, the tool loads in all Windows OS drivers named "win32dd.sys" or "win64dd.sys", in order to image the memory using the win32dd or win64dd utilities. In all operating systems, triageIR creates a "commands.log" file in the windows drive, which contains a limited log of the executed commands.

Against the above discussion, we conclude that all modifications are justifiable, of a limited extent and can be explained and eventually defended in court.

7.2. TR3Secure

TR3Secure presents an almost consistent behavior in all operating systems it is executed in. Similar to TriageIR, the utilities invoked by TR3Secure result to altering Windows OS components such as Prefetch files. This also appears in some cases (Windows XP, Windows 7 64-bit – SP and no SP -, Windows 8 32- and 64-bit) with temp and recent activity files. In all operating systems TR3Secure loads drivers (sysinternals' PROCEXP141.SYS, mandiant tools driver, Nirsoftopened files driver) in certain folders (c:\windows\system32\drivers, C:\Windows\SysWOW64\), alters or adds registry keys, creates or modifies C:\Windows\WindowsUpdate.log and modifies C:\WINDOWS\Software Distribution\ folder. In Windows 7 and 8, where utilities such as "uptime" and "pslist" fail to execute, appcrash reports are created in specific folders (C:\users\all users\Microsoft\Windows\WER\ReportArchive\ and C:\users\user\-AppData\Local\Microsoft\Windows\WER\ReportArchive\). Finally in Windows 8, folder C:\Windows\INF\ is modified.

Similar to TriageIR, we conclude that all modifications are justifiable, of a limited extent and can be explained and eventually defended in court.

7.3. Kludge 3.20110223

Kludge network edition does not respect ACPO Principle 2 because the changes that it makes to the examined system are extensive, as incident data and called utilities are firstly written in the C:\Windows\Temp folder of the system under investigation. Considering that modern computer systems have at least 512 MB, more than 512 MBs are written to the hard disk of the examined system, as Kludge executes. Thus, although the modifications to the examined system are explainable, they are not justifiable and thus not acceptable. However the modified version of Kludge, respects Principle 2.

In detail, in all operating systems Kludge alters or adds registry keys, creates files in C\Windows\system32\CatRoot2\ folder, attempts to create at least one driver (sysinternals PROCEXP.SYS) in certain folders (c:\windows\system32\drivers, C:\Windows\SysWOW64\) and modifies Prefetch as well as the users' recent activity and temp files. In Windows 7 family appcrash reports are created in specific folder (C:\users\all users\Microsoft\Windows\WER\ReportArchive\) as specific utilities (hobocopy and streams) called by Kludge fail.

8. Suggestions

The triage tools need to have two types of dynamically adjusting behavior:

1. Before the acquisition in order to operate correctly and minimize the risks of errors. This is similar to the make config command in Linux systems, which inspects the variables, paths and other dependencies in a system.
2. During execution, in order to maximize their effectiveness and purpose. For example, forking of unrelated utilities not affecting one another may reduce the triage period. In addition, the invocation of utilities could be modified depending on the acquired data (for example if a suspicious network connection is discovered it may be worthwhile to also capture the traffic).

By observing the behavior of the three tools it seems that disabling Prefetch on Windows systems is a highly advised action since this will result to less system alterations. This can be achieved by modifying the registry value controlling Prefetch, and upon completion the tool must restore the registry key to its' original value (see Appendix B). Registry modifications when done in a controlled manner are more easily justifiable than alterations caused when Prefetch is enabled and such tradeoff seems to be unquestionable. Additionally, the execution speed of robocopy can be increased by using the "XJ" switch ("ex. robocopy.exe %sys_drive% %vol_outpath%\preserved-windowspartitionlog-files\ *.evt *.log *.evtx /S /ZB /copy:-DATSOU /r:1 /w:1 /ts /FP /np /XJ") to exclude junctions from the robocopy file collection, as junctions might lead to creation of nested triage data. Furthermore, it is suggested that the tools keep a detailed log of all actions performed including, if possible, errors produced during execution, as traceability of the tools' execution is a very important part of the forensic process. Moreover, it is recommended that the tools record and undo all registry changes, which they knowingly perform to the examined system.

It is also advisable that all triage tools include functionality for collecting internet activity artifacts (history, cookies, archived passwords, etc.) pertaining to all known browsers.

8.1. TriageIR 0.79

The tool is not Windows 8-ready. Additionally, the tool must have been designed with a specific environment in mind as it predicts triage collection (for specific evidence items) in the specialized winxpe OS environment (destined

to "*enable rapid development of the most reliable and full-featured connected devices*") but not in Windows XP 64-bit.

8.2. TR3Secure

The tool needs to be adjusted in order to be better compatible with Windows 64bit OS, thus it is recommended that the code is modified and more utilities are included, which will cover the 64 bit OS aspect. Additionally, the tool will benefit if it is modified in order to be able to collect registry files, scheduled tasks, peripherals, installed printers, user logons and internet activity artifacts.

8.3. Kludge 3.20110223

The tool was built for specific situations, which's why it searches for certain Antivirus products and why the author of the tool has commented certain lines of code which point out to rootkit scan with Sophos Anti-rootkit and GMER. Additionally, the tool must be modified, in order for it to run from a USB stick or an external drive and save the results there. Moreover, some tools need to be replaced in order to run in Windows 7 and 8.

9. Discussion and future work

We empirically confirmed that by far there is no silver bullet for an all-purpose, highly effective, robust triage tool. Such conclusion was intuitively expected due to the high variety and complexity of modern computer systems. As the complexity is not expected to decrease, and variety in the users' needs and user practices in terms of software and processes will tend to be pluralistic, we recommend the following considerations a first responder should include in order to manage risk and handle uncertainty surrounding a triage phase:

- Maintain a profile of the capabilities of the tools. This profile can consist of a number of qualitative and quantitative metrics and will assist the responder to select the most appropriate tool for the occasion through an informed decision. From the empirical study of the three tools, we propose the following metrics:
  - *Effectiveness.* This refers to the effectiveness metric introduced in Section 4 and captures the ability of the tool to collect a large variety of different incident data. This can be either a qualitative (i.e. on an ordinal descriptive scale of "low"/"medium"/"high") or a quantitative metric (number of types of evidence collected as a percentage of a total number of evidence).
  - *(Un)reliability.* This metric refers to the amount of errors the tool produces. This can be quantitative and described by two values, the mean of the percentages of failed utility executions to total number of executions, and the standard deviation. This metric can be further specified by OS.
  - *Invariability.* Invariability shows whether the tool behaves consistently across different systems. This can be a result of a statistical test.

Some intuitive relations may exist between the metrics. For example, it is expected that an effective and highly reliable tool will have low invariability, since in order for it to have an outstanding performance with a particular OS it will not perform as well when applied to other operating systems. Relationships and utilization strategies of these metrics are part of our future research.

- One of the advantages of using open source tools is that the first responder will have the opportunity to prepare well in advance by modifying himself the tool, in order to fit his needs. This would be particularly useful if there is detailed advanced knowledge on the systems to be seized and may help overcome potential limitations (say a limited RAM in an embedded system, prohibiting the use of a large tool). However, it should be highlighted that this will require a significant amount of programming knowledge on the tool's software technology. Open source approaches are a double-edge sword; although they give a significant amount of control to the user, the final product may not have been extensively tested and verified for various errors that can lead to catastrophic situations during a triage exercise. In any case, the competent examiner must modify the tool keeping in mind a list of desirable properties and characteristics the tool should maintain (see for example the work by Mislan et al. (2010) for a comprehensive list of requirements for triage inspection tools).

Another point is the need of having a portfolio of triage tools, for the reason that some tools may be recognized as viruses from the installed antivirus software and as such their execution may be hindered. In situations where the execution of a triage tool is affected by the antivirus, the first responder's alternatives are: a) disable the antivirus software, b) use a different tool and c) have an obfuscated version of the tool. Alternative (a) would be the preferable alternative in most situations as the changes to the suspect system can be well documented (ACPO Principles 2 and 3) and at the same time the most preferable to the first responder tool will be employed. We consider alternative (c) to be the least preferable action because it requires a higher degree of preparation. In addition, despite the fact that there are obfuscation tools that trivially transform the executable code to another congruent form, yet there is no guarantee that the code will be fully compatible with the original one and that it will still not be detected by the antivirus.

In our future research effort we plan to revisit the tools and assess them from a usefulness and quality perspective, to determine if the triage data collected are immediately exploitable by the examiner and if they provide valuable information on a case-by-case basis. Subsequently, our goal is to build our own triage tool that combines useful functionality from all three tested tools and produces, in a case-by-case basis, results that enhance the triage process.

Appendix A. Modifications and improvements performed on the triage tools

A.1. Kludge

This tool is designed to run remotely to target host using administrative shares. We modified the script, in order to

run it locally. It can be downloaded from http://isir.ee.duth.gr/?p=243.

A.2. TR3Secure

We performed the following modifications:

- In line 179 (“*tools|robocopy.exe %WINDIR%|Prefetch %c_drive%:|Data-%case%|%computername%-%timestamp%|preserved-prefetch-files|Prefetch| /ZB /copy:DTSOU /r:4 /w:1 /ts /FP /np /log:%c_drive%:|Data-%case%|%computername%-%timestamp%|preserved-prefetch-files|pretch-robocopy-log.txt)*”) the tool was missing a robocopy copy parameter and it had an unneeded parentheses in the end of the command. The correct command would be “*tools|robocopy.exe %WINDIR%|Prefetch %c_drive%:|Data-%case%|%computername%-%timestamp%|preserved-prefetch-files|Prefetch| /ZB /copy:DATSOU /r:4 /w:1 /ts /FP /np /log:%c_drive%:|Data-%case%|%computername%-%timestamp%|preserved-prefetch-files|pretch-robocopy-log.txt*”. We modified the line in question.
- In line 271 the command should be “*tools|pv.exe -e >> %vol_outpath%|ProcessInfo_2_process-to-exe-mapping.txt*” and not “*tools|pvc.exe -e >> %vol_outpath%|ProcessInfo_2_process-to-exe-mapping.txt*”. We modified the command accordingly.
- in lines 273–281 the Currprocess tool runs as CProcess.exe (when downloaded) not currprocess.exe. We replaced all occurrences of currprocess.exe with cprocess.exe.
- In windows 7 64 bit the tool could not find the path of the “tools” folder, thus we had to add the following parameters:

SET mypath=%~dp0
%mypath:~0,-1%

Appendix B. Suggestions

The following .bat script excerpt will disable Prefetch prior to running any triage tool. The excerpt can be ported, as is, in the TR3Secure triage tool. In other triage tools, the excerpt needs to be adjusted accordingly.

```
:: declaring variables used for prefetcher value
Set original_prefetch_value=""
Set "RegKey=HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters"
Set "RegItem=EnablePrefetcher"
:: querying the original prefetcher value
echo executing Reg query "%RegKey%" /v "%RegItem%" to capture original prefetcher value
For /F "Tokens=2*" %%a in ('Reg query "%RegKey%" /v "%RegItem%"') Do set
original_prefetch_value=%%b
::on first run disable prefetch through registry to avoid executed tools being stored in prefetch and
modifying the hard disk
echo %DATE% %TIME% - Executing reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters" /v EnablePrefetcher /t REG_DWORD /d 0 /f  to disable prefetch
for computer %COMPUTERNAME% >> Collection.log
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters" /v EnablePrefetcher /t REG_DWORD /d 0 /f

:: triage tool is run at this point

::on exit re-enable prefetch through registry to return system to original prefetch state
echo %DATE% %TIME% - Executing reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters" /v EnablePrefetcher /t REG_DWORD /d
%original_prefetch_value% /f  to re-enable prefetch for computer %COMPUTERNAME% >>
Collection.log
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\PrefetchParameters" /v EnablePrefetcher /t REG_DWORD /d
%original_prefetch_value% /f
```

Appendix C. Forensic soundness and impact of tools

The following representative excerpts were extracted from the sandbox analyzer reports. Multiple entries are omitted for brevity.

C.1. Kludge

Windows XP SP3:
[Changes to filesystem]
None
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Explorer\BitBucket
HKEY_CURRENT_USER\software\Sysinternals\… [multiple entries]

Win 7 and Win 7 64 bit:
[Changes to filesystem]
Creates file C:\Users\user\AppData\Local\Temp\REGC92D.tmp
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Explorer\BitBucket\
HKEY_CURRENT_USER\software\Sysinternals\
HKEY_CURRENT_USER\software\classes\Local Settings\-Software\Microsoft\Windows\Shell\MuiCache\C:\Windows\System32

Win 8 32 bit:
[Changes to filesystem]
Creates file C:\Users\user\AppData\Local\Temp\REG8D61.tmp
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Explorer\BitBucket

Win 8 64 bit:
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Explorer\BitBucket
HKEY_CURRENT_USER\software\Sysinternals

C.2. TR3Secure

Win XP SP3
[Changes to filesystem]
C:\WINDOWS\Prefetch\… [multiple files]
C:\WINDOWS\SoftwareDistribution\DataStore\… [multiple files]
C:\WINDOWS\system32\Drivers\PROCEXP141.SYS
C:\WINDOWS\WindowsUpdate.log
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
[Changes to registry]
HKEY_LOCAL_MACHINE\software\… [multiple entries]
HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\… [multiple entries]
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\…
HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\…
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\ShellNoRoam\MUICache

Win 7 64 bit:
[Changes to filesystem]
C:\Windows\SoftwareDistribution\DataStore\… [multiple files]
C:\WINDOWS\WindowsUpdate.log
[Changes to registry]
HKEY_LOCAL_MACHINE\software\Classes\… [multiple entries]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\… [multiple entries]
HKEY_CURRENT_USER\software\Microsoft\… [multiple entries]
HKEY_CURRENT_USER\software\Classes\… [multiple entries]

Win 7 32 bit:
[Changes to filesystem]
C:\Windows\Prefetch\… [multiple files]
C:\Windows\SoftwareDistribution\DataStore\… [multiple files]
C:\Windows\system32\Drivers\PROCEXP141.SYS
C:\Windows\WindowsUpdate.log
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_uptime.exe_c4f252339dafdfe57a4768ce31c665d7e7ee3b2a_09806732\Report.wer
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\… [multiple entries]
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\… [multiple entries]
HKEY_CURRENT_USER\software\Microsoft\… [multiple entries]
HKEY_CURRENT_USER\software\Sysinternals\… [multiple entries]
HKEY_CURRENT_USER\software\classes… [multiple entries]

Win 8 64 bit:
[Changes to filesystem]
C:\Windows\INF\… [multiple files]
C:\Windows\SoftwareDistribution\… [multiple files]
[Changes to registry]
HKEY_LOCAL_MACHINE\software\Classes\… [multiple entries]
HKEY_LOCAL_MACHINE\software\microsoft\SQMClient\Windows\DisabledProcesses
HKEY_LOCAL_MACHINE\software\microsoft\TelemetryClient\SampleStore\
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\… [multiple entries]
HKEY_LOCAL_MACHINE\software\Policies\Microsoft\Windows\IPSEC\Policy\Local

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\…[multiple entries]
HKEY_CURRENT_USER\software\Microsoft\ResKit\…[multiple entries]
HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\…[multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\MuiCache\…[multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\…[multiple entries]

Win 8 32 bit:
[Changes to filesystem]
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Prefetch\…[multiple entries]
C:\Windows\SoftwareDistribution\DataStore\Logs\edb.chk
C:\Windows\system32\CatRoot2\edb.chk
C:\Windows\system32\Drivers\PROCEXP141.SYS
C:\Windows\WindowsUpdate.log
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_uptime.exe_c4f252339dafdfe57a4768ce31c665d7e7ee3b2a_18f9d32c\Report.wer
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\…[multiple entries]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\Windows Error Reporting\…[multiple entries]
HKEY_LOCAL_MACHINE\software\Policies\Microsoft\Windows\IPSEC\Policy\Local
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\…[multiple entries]
HKEY_CURRENT_USER\software\Microsoft\ResKit\…[multiple entries]
HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\…[multiple entries]
HKEY_CURRENT_USER\software\Microsoft\Windows\Windows Error Reporting \…[multiple entries]
HKEY_CURRENT_USER\software\Sysinternals\…[multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\MuiCache\…[multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\…[multiple entries]

C.3. TriageIR

Win XP SP3
[Changes to filesystem]
C:\commands.log
C:\Windows\Prefetch\…[multiple files]
C:\WINDOWS\system32\CatRoot2\…[multiple files]
C:\WINDOWS\system32\WBEM\Logs\mofcomp.log
C:\Documents and Settings\Administrator\Application Data\Microsoft\CryptnetUrlCache\…[multiple files]
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Explorer\BitBucket
HKEY_LOCAL_MACHINE\software\microsoft\WBEM\WMIC
HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\… [multiple entries]
HKEY_LOCAL_MACHINE\software\microsoft\SystemCertificates\AuthRoot\Certificates\… [multiple entries]
HKEY_CURRENT_USER\software\Sysinternals\…[multiple entries]

Win 7 32 bit
[Changes to filesystem]
C:\commands.log
C:\Windows\Prefetch\… [multiple files]
C:\Windows\system32\CatRoot2\edb.chk
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache… [multiple files]
[Changes to registry]
HKEY_LOCAL_MACHINE\software\microsoft\… [multiple entries]
HKEY_LOCAL_MACHINE\System\CurrentControlSet\… [multiple entries]
HKEY_CURRENT_USER\software\Microsoft\… [multiple entries]
HKEY_CURRENT_USER\software\classes\… [multiple entries]

Win 7 64 bit
[Changes to filesystem]
C:\commands.log
C:\Windows\Prefetch\… [multiple files]
C:\Windows\system32\winevt\Logs… [multiple .evtx files]
[Changes to registry]
HKEY_LOCAL_MACHINE\software\Classes\CLSID\… [multiple entries]
HKEY_LOCAL_MACHINE\software\Classes\Protocols\… [multiple entries]
HKEY_LOCAL_MACHINE\software\Classes\Wow6432Node\… [multiple entries]
HKEY_LOCAL_MACHINE\software\microsoft\… [multiple entries]
HKEY_LOCAL_MACHINE\System\CurrentControlSet\… [multiple entries]
HKEY_CURRENT_USER\software\Sysinternals\… [multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\… [multiple entries]

Win 8 32 bit
[Changes to filesystem]
C:\commands.log
C:\Windows\Prefetch\… [multiple files]
C:\Windows\system32\CatRoot2\edb.chk
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\… [multiple files]
[Changes to registry]

HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Explorer\BitBucket
HKEY_LOCAL_MACHINE\software\Policies\Microsoft\-Windows\… [multiple entries]
HKEY_CURRENT_USER\software\Sysinternals\… [multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\… [multiple entries]

Win 8 64 bit:
[Changes to filesystem]
C:\commands.log
C:\Windows\Prefetch\… [multiple files]
C:\Windows\system32\CatRoot2\edb.chk
C:\Windows\system32\winevt\Logs\… [multiple files]
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\… [multiple files]
[Changes to registry]
HKEY_LOCAL_MACHINE\software\Classes\… [multiple entries]
HKEY_LOCAL_MACHINE\software\microsoft\… [multiple entries]
HKEY_LOCAL_MACHINE\software\Policies\Microsoft\Windows\IPSEC\Policy\Local
HKEY_LOCAL_MACHINE\software\Wow6432Node\Microsoft\RFC1156Agent\CurrentVersion\Parameters
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDlls
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\… [multiple entries]
HKEY_CURRENT_USER\software\Microsoft\ResKit\… [multiple entries]
HKEY_CURRENT_USER\software\Microsoft\Windows\-CurrentVersion\Explorer\BitBucket\… [multiple entries]
HKEY_CURRENT_USER\software\Sysinternals\… [multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\MuiCache\… [multiple entries]
HKEY_CURRENT_USER\software\classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\… [multiple entries]

References

7Zip Command Line, http://www.7-zip.org/.
ACPO. Good practice guide for computer-based electronic evidence. http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf; 2008.
Aljaedi A., Lindskog D., Zavarsky P., Ruhl R., Almari F. Comparative analysis of volatile memory forensics: live response vs. memory imaging. In: Proceedings of the 2011 IEEE third international conference on and 2011 IEEE third international conference on Social Computing (SocialCom), 2011 9–11 Oct., Boston, MA, USA, pp. 1253–1258.
Brezinski D, Killalea T. Guidelines for evidence collection and archiving. RFC 3227, http://www.ietf.org/rfc/rfc3227.txt; 2002.
Brownlee N, Guttman E. Expectations for computer security incident response. RFC 2350, http://www.ietf.org/rfc/rfc2350.txt; 1998.
Buster Sandbox Analyzer (BSA), http://bsa.isoftware.nl/.
DumpIt memory utility, http://www.moonsols.com/windows-memory-toolkit/.
ForensicArtifacts.com, http://forensicartifacts.com/.
Free Merriam-Webster dictionary, http://www.merriam-webster.com/dictionary/.
Hobocopy utility, https://github.com/candera/hobocopy/downloads.
Horsman G., Laing C., Vickers P. A case based reasoning system for automated forensic examinations. In: PGNET 2011, the 12th annual postgraduate symposium on the convergence of telecommunications, networking and broadcasting, 27–28 June, 2011, Liverpool. http://www.cms.livjm.ac.uk/pgnet2011/Proceedings/Papers/m1569452341-horsman.pdf.
Kludge-3.20110223, http://theinterw3bs.com/?p=503.
Lee R. Sans DFIR Faculty. Sans-Digital-Forensics-and-Incident-Response-Poster-2012. http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf; 2012.
Md5deep and sha1deep utilities, http://md5deep.sourceforge.net/.
Mislan R, Casey E, Kessler G. The growing need for on-scene triage of mobile devices. Digital Investigation 2010;6(3–4):112–24.
Netmarketshare, Market share statistics for internet technologies, http://www.netmarketshare.com/ [accessed 31.12.12.].
Nirsoft web browsers tools package, http://www.nirsoft.net/web_browser_tools.html.
OPSWAT. Antivirus market analysis. http://www.opswat.com/about/media/reports/antivirus-december-2012; December 2012.
Pearson S, Watson R. Digital Triage Forensics: processing the digital crime scene. Syngress; 2010.
RegRipper, http://code.google.com/p/winforensicaanalysis/downloads/list.
Rogers M.K., Goldman J., Mislan R., Wedge T., Debrota S. Computer forensics field triage process model. In: Proceedings of the conference on Digital Forensics, Security and Law, 2006 April 20–21, Las Vegas, Nevada, USA, pp. 27–40. http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006-CFFTPM.pdf.
Sandboxie, http://www.sandboxie.com, http://www.sandboxie.com/index.php?AllPages.
Skoudis E. Windows Command-Line Kung Fu with WMIC. http://isc.sans.edu/diary/Windows+Command-Line+Kung+Fu+with+WMIC/1229; 2006, March, 30.
SPEKTOR triage tool, http://www.evidencetalks.com/index.php?option=com_content&view=category&layout=blog&id=83&Itemid=513.
Sysinternals Suite, http://technet.microsoft.com/en-us/sysinternals/bb84206.
TR3Secure, http://code.google.com/p/jiir-resources/downloads/detail?name=tr3secure_data-collection-script.zip&can=2&q=.
TriageIR v.79, http://code.google.com/p/triage-ir/downloads/list.
Waits C, Akinyele JA, Nolan R, Roggers L. Computer forensics: results of live response inquiry vs. memory image analysis. TECHNICAL NOTE CMU/SEI-2008-TN-017. CERT Digital Intelligence and Investigation Directorate (DIID), CarnegieMellon, http://www.cert.org/archive/pdf/08tn017.pdf; 2008.
Windows XP Embedded (WinXPe) OS, http://www.microsoft.com/windowsembedded/en-us/develop/windows-xp-embedded-for-developers.aspx.